REMARKS

Applicants respectfully request reconsideration of the above referenced patent application in view of the amendments and remarks set forth herein, and respectfully request that the Examiner withdraw all rejections. Claims 1, 11, 22 and 29 have been amended. No claims have been canceled. No claims have been added. Thus, claims 1-5, 7-33 and 35-38 are pending.

35 U.S.C. §103(a) Rejections

Claims 1-4, 11, 13-16, 18-20, 22, 24-27, 29 and 30-32

The Advisory Action mailed September 29, 2009 (hereinafter "Advisory Action") maintains the 35 U.S.C. §103(a) rejection of these claims in the Final Office Action mailed July 06, 2009 (hereinafter "Final Office Action), which alleges that the claims are obvious over Davis et al., US Pat. App. No. 2005/0076228 (hereinafter "*Davis*") in view of Ravi et al., US Pat. App. No. 2005/0204155 (hereinafter "*Ravi*") in further view of Remer et al., USPN 7,076,653 (hereinafter "*Remer*") and in further view of Cromer et al., US Pat. App. No. 2005/0166213 (hereinafter "*Cromer*"). For at least the following reasons, Applicants traverse the above rejection.

Applicants respectfully submit that each of the above rejected claims is not obvious in light of *Davis, Ravi, Remer* and *Cromer*, based at least on the failure of the references to teach or suggest (emphasis added):

> "…**the one of the clients detecting a message requesting a secure network connection** for the encrypted traffic flow,
>
> **in response to detecting the message**, the embedded agent of the one of the clients **verifying, prior to any allowing of the requested secure network connection**, that a platform of the one of the clients is not in a compromised state at a time before providing access to the encrypted traffic flow,…"

as variously recited in current independent claims 1, 11, 22 and 29. The claim amendments are supported in the original disclosure at least by FIG. 5 and by paragraphs [0050]-[0052] of the specification.

The Final Office Action relies upon *Davis* paragraphs [0038] and [0042] as allegedly teaching verifying, prior to any allowing of a requested secure connection, that a platform of the one of multiple clients is not in a compromised state at a time before providing access to an encrypted traffic flow. The relied upon passages relate generally to an authentication input device 136 – e.g. a smart card – of a security processing system 102 enabling authentication of a user attempting to access a host processor 130 of the security processing system 102. See, e.g. *Davis* paragraph [0038]. More particularly, the Advisory Action alleges that the claimed verifying prior to any allowing of a requested secure connection is taught by "a form of mutual hardware authentication" (Advisory Action, "Continuation of 11", last paragraph) between authentication input device 136 and host processor 130.

Without agreeing as to whether *Davis* discloses the alleged mutual hardware authentication, Applicants note that *Davis* fails to provide any indication as to **when any such mutual hardware authentication might be performed**. More particularly, *Davis* fails to teach or suggest whether or how any mutual hardware authentication by authentication input device 136 and host processor 130 might by **performed in response to some detecting of a message requesting a secure network connection**. Nor does *Davis* teach verifying that a platform of a client is not in a compromised state, where the verifying is both in response to detecting a message requesting a secure network connection and prior to any allowing of the requested secure network connection.

By contrast, current independent claims 1, 11, 22 and 29 variously recite one of multiple clients detecting **a message requesting a secure network connection** and verifying that a platform of the one of the clients is not in a compromised state at a time before providing access to an encrypted traffic flow, **the verifying in response to detecting the message** and prior to any allowing of the requested secure network connection. The claim rejection does not offer any of *Ravi*, *Remer* and/or *Cromer* as curing the failure of *Davis* to teach verifying a client platform is not in a compromised state, the verifying in response to request for a secure network connection and prior to any allowing of the requested secure network connection. Applicants respectfully submit that no such verifying is taught or suggested by any combination of *Davis*, *Ravi*, *Remer* and *Cromer*.

Even assuming *arguendo* that all other limitations are obvious in view of *Davis*, *Ravi*, *Remer* and *Cromer*, which Applicants do not agree, the references nevertheless fail to teach or suggest at least one limitation of the invention as variously recited in each of independent claims 1, 11, 22 and 29. Accordingly, each of independent claims 1, 11, 22 and 29 is non-obvious in light of *Davis, Ravi, Remer* and *Cromer*, as are any claimed depending therefrom. For at least the foregoing reasons, Applicants request that the above 35 U.S.C. §103(a) rejection of claims 1-4, 11, 13-16, 18-20, 22, 24-27, 29 and 30-32 based on *Davis, Ravi, Remer* and *Cromer* be withdrawn.

Claims 5 and 33

These claims are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable in view of *Davis*, *Ravi*, *Remer*, *Cromer* and in further view of Yokota et al., US Pat. App. No. 2002/0164035 (hereinafter "*Yokota*"). For at least the following reasons, Applicants traverse the above rejection.

As demonstrated in the discussion above, there is at least one limitation in each of current independent claim 1, 11, 22 and 29 which is not taught or suggested by *Davis*, *Ravi*, *Remer* and *Cromer*. *Yokota*, which generally relates to the distribution and management of cryptographic keys, does not cure the failure of *Davis*, *Ravi*, *Remer* and *Cromer* to teach or suggest verifying that a platform of a client is not in a compromised state, where the verifying is both in response to detecting a message requesting a secure network connection and prior to any allowing of the requested secure network connection. Therefore, even assuming *arguendo* that all other limitations are obvious in view of *Davis*, *Ravi*, *Remer*, *Cromer* and *Yokota*, which Applicants do not agree, the references nevertheless fail to teach or suggest at least one limitation of the invention as variously recited in each of independent claims 1, 11, 22 and 29.

Accordingly, each of independent claims 1, 11, 22 and 29 – and any claims depending therefrom – is non-obvious in light of *Davis*, *Ravi*, *Remer*, *Cromer* and *Yokota*. Applicants respectfully request that the above 35 U.S.C. §103(a) rejection of claims 5 and 33 based on *Davis*, *Ravi*, *Remer*, *Cromer* and *Yokota* be withdrawn.

Claims 9 and 37

These claims are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Davis*, *Ravi*, *Remer*, *Cromer* and in further view of Walker et al., US

Pat. App. No. 2002/0163920 (hereinafter "*Walker*"). For at least the following reasons, Applicants traverse the above rejection.

As demonstrated in the discussion above, there is at least one limitation in each of current independent claim 1, 11, 22 and 29 which is not taught or suggested by *Davis*, *Ravi*, *Remer* and *Cromer*. *Walker*, which generally relates to techniques for routing packets according to a security association (SA), does not cure the failure of *Davis*, *Ravi*, *Remer* and *Cromer* to teach or suggest verifying that a platform of a client is not in a compromised state, where the verifying is both in response to detecting a message requesting a secure network connection and prior to any allowing of the requested secure network connection. Therefore, even assuming *arguendo* that all other limitations are obvious in view of *Davis*, *Ravi*, *Remer*, *Cromer* and *Walker*, which Applicants do not agree, the references nevertheless fail to teach or suggest at least one limitation of the invention as variously recited in each of independent claims 1, 11, 22 and 29.

Accordingly, each of independent claims 1, 11, 22 and 29 is non-obvious in light of *Davis*, *Ravi*, *Remer*, *Cromer* and *Walker*, as are any claims depending therefrom. For at least the foregoing reasons, Applicants request that the above 35 U.S.C. §103(a) rejection of claims 9 and 37 based on *Davis*, *Ravi*, *Remer*, *Cromer* and *Walker* be withdrawn.

Claims 10, 17, 28 and 38

These claims are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Davis*, *Ravi*, *Remer*, *Cromer* and in further view of Ylonen, USPN 6,782,474 (hereinafter "*Ylonen*"). For at least the following reasons, Applicants traverse the above rejection.

As demonstrated in the discussion above, there is at least one limitation in each of current independent claim 1, 11, 22 and 29 which is not taught or suggested by *Davis*, *Ravi*, *Remer* and *Cromer*. *Ylonen*, which generally relates to network configuration using device-specific configuration packets, does not cure the failure of *Davis*, *Ravi*, *Remer* and *Cromer* to teach or suggest verifying that a platform of a client is not in a compromised state, where the verifying is both in response to detecting a message requesting a secure network connection and prior to any allowing of the requested secure network connection. Therefore, even assuming *arguendo* that all other limitations are obvious in view of *Davis*, *Ravi*, *Remer*, *Cromer* and *Ylonen*, which Applicants do not agree, the references nevertheless fail to teach or suggest at least one limitation of the invention as variously recited in each of independent claims 1, 11, 22 and 29.

Accordingly, each of independent claims 1, 11, 22 and 29 is non-obvious in light of *Davis*, *Ravi*, *Remer*, *Cromer* and *Ylonen*, as are any claims depending therefrom. For at least the foregoing reasons, Applicants request that the above 35 U.S.C. §103(a) rejection of claims 10, 17, 28 and 38 based on *Davis*, *Ravi*, *Remer*, *Cromer* and *Ylonen* be withdrawn.

Claims 12 and 23

These claims are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Davis*, *Ravi*, *Remer*, *Cromer* and in further view of Grohoski et al., US Pat. App. No. 2004/0225885 (hereinafter "*Grohoski*"). For at least the following reasons, Applicants traverse the above rejection.

As demonstrated in the discussion above, there is at least one limitation in each of current independent claim 1, 11, 22 and 29 which is not taught or suggested by *Davis*, *Ravi*, *Remer* and *Cromer*. *Grohoski*, which generally relates to use of a cryptographic co-processor, does not cure the failure of *Davis*, *Ravi*, *Remer* and *Cromer* to teach or suggest verifying that a platform of a client is not in a compromised state, where the verifying is both in response to detecting a message requesting a secure network connection and prior to any allowing of the requested secure network connection. Therefore, even assuming *arguendo* that all other limitations are obvious in view of *Davis*, *Ravi*, *Remer*, *Cromer* and *Grohoski*, which Applicants do not agree, the references nevertheless fail to teach or suggest at least one limitation of the invention as variously recited in each of independent claims 1, 11, 22 and 29.

Accordingly, each of independent claims 1, 11, 22 and 29 is non-obvious in light of *Davis*, *Ravi*, *Remer*, *Cromer* and *Grohoski*, as are any claims depending therefrom. For at least the foregoing reasons, Applicants request that the above 35 U.S.C. §103(a) rejection of claims 12 and 33 based on *Davis*, *Ravi*, *Remer*, *Cromer* and *Grohoski* be withdrawn.

Claim 21

This claims is rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Davis*, *Ravi*, *Remer*, *Cromer* and in further view of Kramer et al., US Pat. App. No. 2005/0201554 (hereinafter "*Kramer*"). For at least the following reasons, Applicants traverse the above rejection.

As demonstrated in the discussion above, there is at least one limitation in each of current independent claim 1, 11, 22 and 29 which is not taught or suggested by *Davis*, *Ravi*, *Remer* and *Cromer*. *Kramer*, which generally relates to encryption techniques using a cipher counter, does not cure the failure of *Davis*, *Ravi*, *Remer* and *Cromer* to teach or suggest verifying that a platform of a client is not in a compromised state, where the verifying is both in response to detecting a message requesting a secure network connection and prior to any allowing of the requested secure network connection. Therefore, even assuming *arguendo* that all other limitations are obvious in view of *Davis*, *Ravi*, *Remer*, *Cromer* and *Kramer*, which Applicants do not agree, the references nevertheless fail to teach or suggest at least one limitation of the invention as variously recited in each of independent claims 1, 11, 22 and 29.

Accordingly, each of independent claims 1, 11, 22 and 29 is non-obvious in light of *Davis*, *Ravi*, *Remer*, *Cromer* and *Kramer*, as are any claims depending therefrom. For at least the foregoing reasons, Applicants request that the above 35 U.S.C. §103(a) rejection of claim 21 based on *Davis*, *Ravi*, *Remer*, *Cromer* and *Kramer* be withdrawn.

CONCLUSION

For at least the foregoing reasons, Applicants submit that the objections and rejections have been overcome. Therefore, claims 1-5, 7-33 and 35-38 are in condition for allowance and such action is earnestly solicited. The Examiner is respectfully requested to contact the undersigned by telephone if such contact would further the examination of the present application. Please charge any shortages and credit any overcharges to our Deposit Account number 02-2666.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP

Date: October 26, 2009

/Dermot G. Miller/
Dermot G. Miller
Attorney for Applicants
Reg. No. 58,309

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(503) 439-8778